TLP:WHITE

ICS Advisory (ICSA-19-183-01)

More ICS-CERT Advisories

Schneider Electric Modicon Controllers

Original release date: July 02, 2019

Legal Notice

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Schneider Electric
- **Equipment:** Modicon Controllers
- **Vulnerability:** Improper Check for Unusual or Exceptional Conditions

2. RISK EVALUATION

Successful exploitation of this vulnerability could result in a denial-of-service condition.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Modicon Controllers, a PLC and PAC controller for industrial control systems, are affected:

- Modicon M340: Firmware versions prior to v3.01
- Modicon M580: Firmware versions prior to v2.80
- Modicon Quantum: All firmware versions
- Modicon Premium: All firmware versions

TLP:WHITE

3.2 VULNERABILITY OVERVIEW

TLP:WHITE

3.2.1 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754

An attacker could create a denial-of-service condition by sending a specific crafted Modbus frame to the affected device.

CVE-2019-6819 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Multiple Sectors
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** France

3.4 RESEARCHER

Zhang Xiaoming, Zhang Jiawei, Sun Zhonghao and Luo bing of CNCERT/CC reported this vulnerability to NCCIC.

4. MITIGATIONS

Schneider Electric has recommended the following to mitigate this vulnerability.

Modicon M340 – The vulnerability is fixed in v3.01 and is available for download below:

- BMXP3420302 and CL and H: https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/
- BMXP342020 and H: https://www.schneider-electric.com/en/download/document/BMXP342020_Firmwares/
- BMXP342000: https://www.schneider-electric.com/en/download/document/BMXP342000_Firmwares/
- BMXP341000 and H: https://www.schneider-electric.com/en/download/document/BMXP341000_Firmwares/
- BMXP3420102 and CL: https://www.schneider-electric.com/en/download/document/BMXP3420102_Firmwares/
- BMXP3420302 and H: https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/

Modicon M580 – The vulnerability is fixed in v2.80 and is available for download below:

- BMEP584040, BMEP584040S, BMEH584040 and C: https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV2.80/
- BMEP586040 and C: https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV2.80/

TLP:WHITE

- BMEH586040 and C: https://www.schneiderelectric.com/en/download/document/M580_BMEH586040_SV2.80/
- BMEP581020 and H: https://www.schneiderelectric.com/en/download/document/M580_BMEP581020_SV2.80/
- BMEP582020 and H: https://www.schneiderelectric.com/en/download/document/M580_BMEP582020_SV2.80/
- BMEP582040 and H: https://www.schneiderelectric.com/en/download/document/M580_BMEP582040_SV2.80/
- BMEP583020: https://www.schneiderelectric.com/en/download/document/M580_BMEP583020_SV2.80/
- BMEP583040: https://www.schneiderelectric.com/en/download/document/M580_BMEP583040_SV2.80/
- BMEP584020: https://www.schneiderelectric.com/en/download/document/M580_BMEP584020_SV2.80/
- BMEP585040 and C: https://www.schneiderelectric.com/en/download/document/M580_BMEP585040_SV2.80/
- BMEP582040S: https://www.schneiderelectric.com/en/download/document/M580_BMEP582040S_SV2.80/
- BMEH582040 and C: https://www.schneiderelectric.com/en/download/document/M580_BMEP582040_SV2.80

Schneider Electric's Modicon Quantum controllers have reached the end of their life and are no longer commercially available. They have been replaced by the Modicon M580 ePAC controller, Schneider Electric's most current product. Schneider Electric recommends users migrate to the Modicon M580 ePAC.

To mitigate risks associated with this Modbus vulnerability, users should immediately set up network segmentation and implement a firewall to block all unauthorized access to Port 502/TCP.

Schneider Electric general security recommendations:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so no unauthorized persons have access to the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the intended devices.
- All methods of mobile data exchange with the isolated network (e.g., CDs, USB drives, etc.) should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.

TLP:WHITE

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

For more information, please see Schneider Electric advisory: SEVD-2019-134-05

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability.

Contact Information

For any questions related to this report, please contact the NCCIC at:

Email: NCCICCUSTOMERSERVICE@hq.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: http://ics-cert.us-cert.gov
or incident reporting: https://ics-cert.us-cert.gov/Report-Incident?

The NCCIC continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

TLP:WHITE